



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/642,685	08/21/2000	Stephen Michael Matyas, Jr.	5577-202	8886

20792 7590 03/30/2004

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER

WU, ALLEN S

ART UNIT PAPER NUMBER

2135

2

DATE MAILED: 03/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/642,685

Applicant(s)

MATYAS, JR. ET AL.

Examiner

Allen S. Wu

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 August 2000.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-43 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 1-43 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 21 August 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
2. Claim 14 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
3. Claim 14 recites the limitation "the second key value" in lines 5-6 of claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.
5. Claims 1 and 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al, US Patent 5,337,357.

As per claim 1, Chou et al discloses controlling installation of software (abstract) comprising: an installation center (central processing center, col 3 In 48-57), the installation center having access to first and second secret values associate with a copy of the software for installation (key k1 and k2, col 3 In 48-

56) an unencrypted installation client, the installation client incorporating the first secret value (key k1, col 3 ln 26-47); and an encrypted portion of the software, wherein the encrypted portion of the software is encrypted with a first key value (K) derived from the first and second secret values (k1 and k2, col 3 ln 26-38 and 48-57, also col 4 ln 5-12); and wherein the unencrypted installation client is configured to receive the second secret value from the installation center (processing center col 3 ln 48-57) to generate the first key value, to decrypt the encrypted portion of the software and to install the software (col 4 ln 4-11).

Chou et al does not explicitly teach an installation server acting as the central processing center. However, Chou et al discloses communication with the processing center and supplying the received information to the computer (col 3 ln 48-67). The office takes official notice that servers for use in computer networks for communicating with client computers is notoriously well known in the art at the time of the applicant's invention. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the teachings of Chou et al to include an installation server in place of the central processing center for communication directly to a client computer because it would have automated the process of obtaining information from the center and therefore lessen the physical tasks done by the client while installing software.

As per claim 10, Chou et al further discloses an installation center (processing center) configured to receive a request for installation of the copy of

the software from the client and provide the second secret value to the client in response to the request for installation of the copy of the software. Chou et al does not explicitly teach receiving and providing from an installation server to an installation client. The office takes official notice that servers for use in computer networks for communicating with client computers is notoriously well known in the art at the time of the applicant's invention. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the teachings of Chou et al to include an installation server in place of the central processing center for communication directly to a client computer because it would have automated the process of obtaining information from the center and therefore lessen the physical tasks done by the client while installing software.

As per claim 11, Chou et al does not explicitly teach sending the second secret value to the data processing system if the installation of the copy of the software to be installed is authorized. However, Chou et al discloses a means of prohibiting installation of software by determining if installation is authorized at the computer (col 3 ln 59-col 4 ln 3). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the teachings of Chou et al so that determination of whether installation is authorized occurs at an outside computer (i.e. server) because the applicant has not explicitly stated the purpose of using such determination means and the means disclosed by Chou et al is just as efficient.

6. Claims 2-4, 7, 12-13, 15-17, 19-24, 26-30, and 35-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al, US Patent 5,337,357, in view of Cane et al, US Patent 5,416,840.

As per claims 2 and 17, Chou et al further discloses a need to provide protection in software program distribution (col 1 ln 45-50). However, Chou et al does not explicitly teach the installation client being configured to generate a second key value from the first key value and the first secret value, encrypt the decrypted portion of the software with the second key value and store the portion of the software encrypted with second key value. Cane et al discloses controlling installation of software (abstract), which further encrypts the decrypted portion of the software and stores the encrypted software (col 5 ln 8-19 and col 6 ln 64 – col 7 ln 8). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Cane et al within the system of Chou et al because it would have prevented further distribution of the decrypted software.

Furthermore, the combination of Chou et al and Cane et al does not explicitly teach encrypting the software with a second key. Chou discloses a method where no second key value is the same (col 4 ln 18-37) for the purposes of controlling future installations with the same key. Cane et al further discloses using an authorization code to obtain permission of future use of the software (col 7 ln 9-37). It would have been obvious to one of ordinary skill in the art at

the time of the applicants invention to modify the combination of Chou et al and Cane et al to further encrypt the decrypted portion of the software with a second key value because the applicant has not explicitly stated the purpose of such an encryption other than preventing future installations and the method of encrypting the portion of the software in the combination of Chou et al and Cane et al is just as efficient.

As per claims 3, Chou et al further discloses a need to provide protection in software program distribution (col 1 ln 45-50). Chou et al does not explicitly teach the installation server (processing center) configured to generate the first key value and store the first key value as a subsequent second secret value associated with the copy of the software. Chou et al discloses generating the second secret value based on randomness of first secret value and encryption key (K, col 4ln 17-37). It would have been to one of ordinary skill in the art at the time of the applicant's invention to modify the teachings of Chou et al to further create a second secret value from a first key value because the applicant has not explicitly stated any particular purpose of such a generation other than for prevention of installation on another machine and the means of preventing installation on different computers as disclosed by Chou et al is just as efficient.

As per claim 4 and 28, the combination of Chou et al and Cane et al disclose a means of protecting software installation as described above (see

claim 2). Cane et al further discloses retaining a secret value in addition to a new secret value (authorization code, col 6 ln 64-col 7 ln 36) and selectively supplying the authorization code for access to encrypted software (col 7 ln 9-36). The combination of Chou et al and Cane et al does not explicitly teach the installation server to retain a copy of an initial second secret value associated secret value associated with the copy of the software and to selectively provide the initial second secret value to the installation client. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the combination of Chou et al and Cane et al to further retain a copy of an initial second secret value and to selectively provide the initial second secret value because the applicant has not explicitly stated any particular purpose for such retaining and supplying other than for prevention of unauthorized installation or copying and that the means of the combination of Chou et al and Cane et al is just as efficient.

As per claim 7, the combination of Chou et al and Cane et al discloses an installation client, which is configured to decrypt the encrypted portion of the software and encrypt the portion of the software as described above (see claim 2). Cane et al further discloses performing the tasks without persistently storing key or unencrypted data at the installation client (col 2 ln 55-65 and col 6 ln 45-col 7 ln 8). It is important to keep important to keep the key data and unencrypted data from being persistently stored on an installation client to

prevent unauthorized access to the information. It is well known in the art that storing data persistently on a computer is prone to attacks by outsiders who may be able to obtain such unprotected data. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to further combine the teachings of Chou et al and Cane et al because it would have increased security of software being stolen from a client's system.

As per claim 12, Chou et al does not explicitly teach a network interconnecting the installation server and the installation client. Cane et al discloses a network for broadcasting software (col 4 ln 50-65). Furthermore, the means of interconnecting a server and a client computer in a network is well known in the art and is needed as a means of communicating information from a server computer to a client computer. Therefore it would have been obvious to one of ordinary skill in the art to modify the teachings of Chou et al to further include a network for communication between an installation server and a client computer because it would have provided a means of automated installation through methods well known in the art.

As per claim 13, the combination of Chou et al and Cane et al does not disclose a network comprising the Internet. The office takes official notice that the Internet is notoriously well known in the art at the time of the applicant's invention as a network for communication between computers. It would have

been obvious to one of ordinary skill in the art at the time of the applicant's invention to further modify the combination of Chou et al and Cane et al to use the Internet as a network for communicating between an installation server and an installation client because of the advantages of being to communicate between the server and client worldwide through a network that is well established in the art.

As per claims 15, 39, 41, and 43, Chou et al discloses providing a copy of the software (col 2 ln 40-56), the software being divided into a first encrypted portion and a second unencrypted portion having access to a first secret value (k1) (col 3 ln 26-47) wherein the first encrypted portion is encrypted with a first key value which is based on the first secret value and a second secret value (col 4 ln 5-16); obtaining the second secret value (k2, col 3 ln 48-67), generating the first key value from the obtained second secret value and the first secret value (col 4 ln 4-12) and decrypting the first encrypted portion of the software utilizing the first key value (col 4 ln 5-17).

Furthermore, Chou et al discloses a first and second secret value being associated with the computer (col 3 ln 5-17 and col 3 ln 48-57) and multiple software being distributed and employing different encryption keys for each program (col 3 ln 17-25). Chou et al does not explicitly teach a first secret value and a second secret value associated with the software identification of the copy of the software. Cane et al discloses use of a software identifier for identification

of the software the user wishes to install (col 6 ln 3-15), wherein values are used associated with the software identification to obtain a key for decryption (col 6 ln 17-58). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Cane et al within the system of Chou et al because it would have increased organization of encryption keys when multiple software are distributed to a client.

As per claim 16, Chou et al discloses installation of the software on a data processing system utilizing the decrypted first encrypted portion of the software (col 3 ln 26-29 and col 4 ln 12-17).

As per claim 19 and 29, Chou et al further discloses a processing center configured to receive a request for the second secret value from the client and receiving the second secret value from the processing center in response to the request for the second secret value (col 3 ln 48-58). Chou et al does not explicitly teach a network server. The office takes official notice that servers for use in computer networks for communicating with client computers is notoriously well known in the art at the time of the applicant's invention. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the teachings of Chou et al to include replace the processing center with a network server for communication directly to a client computer because it would

have automated the process of obtaining information from the center and therefore lessen the physical tasks done by the client while installing software.

As per claim 20, Chou et al discloses transmitting a request for a second secret value as described above (see claim 19). Chou et al does not explicitly teach the request containing the identification of the copy of the software. Cane et al discloses use of a software identifier for identification of the software the user wishes to install (col 6 ln 3-15) is transmitted to a network server (col 5 ln 1-8), wherein values are used associated with the software identification to obtain a key for decryption (col 6 ln 17-58). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Cane et al within the system of Chou et al because it would have increased organization of encryption keys when multiple software are distributed to a client.

As per claim 21, Chou et al discloses a request as described above (see claim 20). Chou et al further discloses the request containing the obtained user information (col 3 ln 10-11, the user information is used as the first key value, col 3 ln 59-col 4 ln 38).

As per claim 22, Chou et al further discloses user information comprising at least one of identification of a data processing system on which the software is

to be installed and identification of a user associated with the copy of the software (col 3 ln 10-16).

As per claims 23 and 30, Chou et al further discloses determination if the requested installation is authorized and providing the second secret value to the installation client if the requested installation is authorized and sending the second secret value only if the request for an authorized installation of the copy of the software (col 3 ln 59-col 4 ln 3).

As per claim 24, Chou et al further discloses determination of whether the request is for an authorized installation of the software is based on at least one of the identification of the copy of the software, an identification of a user of the software, an identification of a processing system on which the software is to be installed, and authorized number of installations for the copy of the software and a number of previous installations of the copy of the software (col 3 ln 59-col 4 ln 3).

As per claim 26, Chou et al discloses a method of generating a different second secret value in response to a subsequent request for the second secret value based on randomness (col 3 ln 5-17 and col 4 ln 18-45). Chou et al discloses this as a means for prevention of unauthorized copying and installation of software (col 4 ln 18-37). The combination of Chou et al and Cane et al does

not explicitly teach generating a second key value from the first key value and associating the first key value with the identification of the copy of the software as an updated second secret value. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the teachings of Chou et al to generate the first key value and further associating the key value with a second key value because the applicant has not explicitly stated the purpose of such updating of the second secret value other than for prevention of future copying or installation and the means disclosed by Chou is just as efficient.

As per claim 27, the combination of Chou et al and Cane et al disclose a means of protecting software installation as described above (see claim 17). Cane et al further discloses retaining a secret value in addition to a new secret value (authorization code, col 6 ln 64-col 7 ln 36) and selectively supplying the authorization code for access to encrypted software (col 7 ln 9-36). The combination of Chou et al and Cane et al does not explicitly teach the installation server to maintaining a copy of an initial second secret value associated secret value associated with the copy of the software and to selectively provide the initial second secret value to the installation client. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the combination of Chou et al and Cane et al to further maintain a copy of an initial second secret value and to selectively provide the initial second secret value because the applicant has not explicitly stated any particular purpose for such

retaining and supplying other than for prevention of unauthorized installation or copying and that the means of the combination of Chou et al and Cane et al is just as efficient.

As per claims 35, 40, and 42, Chou et al discloses associating a first and second secret values with a copy of the software (col 4 ln 4-11, first and secret values used for generating key), receiving a request for installation of the software on a data processing system (col 3 ln 42-58); determining the second secret value (col 3 ln 48-58); determining if the installation of the copy of the software to be installed is authorized (col 3 ln 59-col 4 ln 3); and sending the second secret value to the data processing system (col 3 ln 48-63).

Chou et al does not explicitly teach sending the second secret value to the data processing system if the installation of the copy of the software to be installed is authorized. However, Chou et al discloses a means of prohibiting installation of software by determining if installation is authorized at the computer (col 3 ln 59-col 4 ln 3). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the teachings of Chou et al so that determination of whether installation is authorized occurs at an outside computer (i.e. server) because the applicant has not explicitly stated the purpose of using such determination means and the means disclosed by Chou et al is just as efficient.

Chou et al does not explicitly teach associating a software identification with a copy of the software. Cane et al discloses associating a software identification with a copy of the software (col 6 ln 4-15) wherein a request for installation identifies the software identification (col 5 ln 1-8) and a key for decryption is determined that is associated with the software identification (col 6 ln 3-44). Chou et al further discloses multiple software being distributed (ln 18-25). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Cane et al within the system of Chou et al because it would have increased organization of encryption keys when multiple software are distributed to a client.

As per claim 36, Chou et al further discloses determination of whether the request is for an authorized installation of the software is based on at least one of the identification of the copy of the software, an identification of a user of the software, an identification of a processing system on which the software is to be installed, and authorized number of installations for the copy of the software and a number of previous installations of the copy of the software (col 3 ln 59-col 4 ln 3).

As per claim 37, Chou et al further discloses generating a first key value from the first and second secret values associated with the copy of the software (col 4 ln 4-12). Chou et al does not explicitly teach associating the first key value

Art Unit: 2135

with the software identification of the copy of the software as an updated first secret value. However, Chou et al discloses a method of updating a secret value each time a secret value is requested for prevention of repetitive installation (col 4 ln 18-37). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to update the first secret value with the first key value because the applicant has not explicitly stated any particular reason for such an updating other than for prevention of future unauthorized installations and that the means disclosed by Chou et al is just as efficient.

As per claim 38, Chou et al does not explicitly teach associating the first key value with the software identification of the copy of the software as an updated first secret value comprising the step of replacing the first secret value associated with the software identification of the copy of the software with the first key value. However, Chou et al discloses a method of updating a secret value each time a secret value is requested for prevention of repetitive installation (col 4 ln 18-37). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to update the first secret value with the first key value because the applicant has not explicitly stated any particular reason for such an updating other than for prevention of future unauthorized installations and that the means disclosed by Chou et al is just as efficient.

7. Claims 5-6, 25, and 31-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al, US Patent 5,337,357, in view of Cane et al, US Patent 5,416,840, and further in view of Larsson et al, US Patent 5,666,411.

As per claim 5, Chou et al does not explicitly teach maintaining a copy of an original second secret value associated with a first key value. However, Chou et al discloses a means for software protection wherein the second value is generated from a first secret value and a key (col 3 ln 48-58). In the method of Chou et al, the second value is used for generating a decryption key at the client computer (col 4 ln 5-11). Furthermore, Cane et al discloses the method preventing subsequent installation of software (col 5 ln 9-18 and col 6 ln 59-col 7 ln 31). The combination of Chou et al and Cane et al provides copy and access control of software to be installed on a client, which further prevents unauthorized sequential installations. It would have been obvious to one of ordinary skill at the time of the applicant's invention to modify the combination of Chou et al and Cane et al to further store the second secret value at an installation center (processing center) because the applicant has not explicitly stated any other purpose of such storing other than for preventing subsequent installations of the software, and that the means disclosed in the combination of Chou et al and Cane et al is just as efficient.

Furthermore, the combination of Chou et al and Cane et al does not explicitly teach means for limiting the amount of installations. Larsson et al discloses a means of controlling the number of installations allowed for the copy

of the software based on a maximum number of installations (col 9 ln 34-57).

Both Larsson et al and the combination of Chou et al and Cane et al disclose a means of protecting distributed software installation. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Larsson et al within the combination of Chou et al and Cane et al because it would have further protected unauthorized software installation. The need to limit the amount of installations allowed are useful in determining the amount to charge the client for purchase of the software. For example, a client may be charged extra for software, which can be installed on two or more computers (corporate licensing) as opposed to just one.

Furthermore, the combination of Chou et al, Cane et al, and Larsson et al does not explicitly teach controlling the number of installations allowed based on a maximum number of times that the original second secret value may be sent. Larsson et al further discloses a method wherein reinstallation on the same computer is not considered installation and therefore not counted towards the maximum of the number of installations (col 4 ln 14-34 and col 9 ln 18-65). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the combination of Chou et al, Cane et al, and Larsson et al to further control installation of software in association of a maximum number of times the original second secret value may be sent to the installation client because the applicant has not explicitly stated any particular reason for using such control means other than to prevent initial installation of

software, and the control means as disclosed by the combination of Chou et al, Carne et al, and Larsson et al is just as efficient.

As per claim 6, the combination of Chou et al and Cane et al does not explicitly teach tracking the number of times that the copy of the software has been installed and the number of times that the original second secret value is sent to the installation client. However, Larsson et al further discloses tracking the number of times that the copy of the software has been installed (col 9 ln 18-65) and means of preventing installation if the installation results in the number of times that the copy of the software has been installed exceeding the maximum number of software installations (col 9 ln 34-65). Both Larsson et al and the combination of Chou et al and Cane et al disclose a means of protecting distributed software installation. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Larsson et al within the combination of Chou et al and Cane et al because it would have further protected unauthorized software installation. The need to limit the amount of installations allowed are useful in determining the amount to charge the client for purchase of the software. For example, a client may be charged extra for software, which can be installed on two or more computers (corporate licensing) as opposed to just one.

As per claims 25 and 31, the combination of Chou et al and Cane et al does not explicitly teach tracking the number of times that the copy of the software has been installed and the number of times that the original second secret value is sent to the installation client. However, Larsson et al further discloses tracking the number of times that the copy of the software has been installed (col 9 ln 18-65) and means of preventing installation if the installation results in the number of times that the copy of the software has been installed exceeding the maximum number of software installations (col 9 ln 34-65). Both Larsson et al and the combination of Chou et al and Cane et al disclose a means of protecting distributed software installation. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Larsson et al within the combination of Chou et al and Cane et al because it would have further protected unauthorized software installation. The need to limit the amount of installations allowed are useful in determining the amount to charge the client for purchase of the software. For example, a client may be charged extra for software, which can be installed on two or more computers (corporate licensing) as opposed to just one.

As per claim 32, the combination of Chou et al and Cane et al does not explicitly teach re-synchronizing of secret values. However, Chou et al and Cane et al disclose a scheme where the secret values are inherently synchronized by basing the second secret value on the first secret value and the key (col 3 ln 48-

col 4 ln 17). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the combination of Chou et al and Cane et al to resynchronize the secret values because the applicant has not explicitly stated any other purpose of re-synchronizing the secret values other than to prevent error in generation of the decryption key and the means of generating decryption keys by using two secret values is just as efficient.

As per claim 33, the combination of Chou et al and Cane et al does not explicitly teach tracking the number of times that the copy of the software has been installed and the number of times that the original second secret value is sent to the installation client. However, Larsson et al further discloses tracking the number of times that the copy of the software has been installed (col 9 ln 18-65) and means of preventing installation if the installation results in the number of times that the copy of the software has been installed exceeding the maximum number of software installations (col 9 ln 34-65). Both Larsson et al and the combination of Chou et al and Cane et al disclose a means of protecting distributed software installation. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Larsson et al within the combination of Chou et al and Cane et al because it would have further protected unauthorized software installation. The need to limit the amount of installations allowed are useful in determining the amount to charge the client for purchase of the software. For example, a client may be

charged extra for software, which can be installed on two or more computers (corporate licensing) as opposed to just one.

8. Claims 8-9, 18, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al, US Patent 5,337,357, in view of Cane et al, US Patent 5,416,840, and further in view of McCarty, US Patent 5,661,411.

As per claims 8 and 18, the combination of Chou et al and Cane et al disclose a method of protecting software installation as described above (see claim 2). The combination of Chou et al and Cane et al does not explicitly teach replacing the encrypted portion of software with the portion of the software encrypted with the second key value. McCarty discloses a method of software protection (abstract) wherein the encrypted software is replaced with the software encrypted with the second key value (col 12 ln 37-54). Both McCarty and the combination of Chou et al and Cane et al disclose method of protecting software access and installation. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of McCarty within the combination of Chou et al and Cane et al because it would have increased security through the use of multiple keys (see McCarty col 3 ln 5-19).

As per claim 9, the combination of Chou et al and Cane et al does not explicitly teach the encrypted portion of the software comprises a plurality of encrypted blocks. McCarty discloses a plurality of encrypted blocks (col 12 ln 36-

60) wherein an installation client is further configured to sequentially decrypt ones of the plurality of encrypted blocks with the first key value and sequentially encrypt and store the decrypted plurality of encrypted blocks with the second key value, wherein the next of the plurality of encrypted blocks is decrypted after a previous of the plurality of encrypted blocks is encrypted with the second key value and stored (Cipher Block Chaining algorithm, col 5 ln 36-48 and col 12 ln 37-col 13 ln 3). Both McCary and the combination of Chou et al and Cane et al disclose a means or software protection. Furthermore, the use of cipher block chaining algorithm to encrypt and decrypt data is a national standard of encryption and decryption. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of McCary within the system of Chou et al and Cane et al because it would have provided further protection of the software by providing a means of detecting file modification (see McCary col 5 ln 36-48).

As per claim 34, the combination of Chou et al and Cane et al does not explicitly teach the encrypted portion of the software comprises a plurality of encrypted blocks. McCarty discloses a plurality of encrypted blocks (col 12 ln 36-60) wherein the step of decrypting the first encrypted portion of the software comprises decrypting an encrypted block of the plurality of encrypted blocks with the first key value (Cipher Block Chaining algorithm, col 5 ln 36-48 and col 12 ln 37-col 13 ln 3) and wherein the step of encrypting the comprises encrypting the

decrypted block with the second key value (col 12 ln 48-53); wherein the step of storing the first encrypted portion of the software encrypted with the second key comprises storing the block encrypted with the second key value (col 17 ln 23-col 18 ln 12), wherein the block of the plurality of encrypted blocks is decrypted, encrypted and stored before a next block of the plurality of blocks is decrypted encrypted and stored (inherent to the cipher block chaining algorithm). Both McCarty and the combination of Chou et al and Cane et al disclose a means or software protection. Furthermore, the use of cipher block chaining algorithm to encrypt and decrypt data is a national standard of encryption and decryption. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of McCarty within the system of Chou et al and Cane et al because it would have provided further protection of the software by providing a means of detecting file modification (see McCarty col 5 ln 36-48).

9. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al, US Patent 5,337,357, in view of McCarty, US Patent 5,661,411.

As per claim 14, Chou et al discloses a method of protecting software installation as described above (see claim 2). Chou et al does not explicitly teach replacing the encrypted portion of software with the portion of the software encrypted with the second key value. McCarty discloses a method of software protection (abstract) wherein the encrypted software is replaced with the software

encrypted with the second key value (col 12 ln 37-54). Both McCarty and Chou et al disclose a method of protecting software access and installation. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of McCarty within the system of Chou et al because it would have increased security through the use of multiple keys (see McCarty col 3 ln 5-19). The combination of Chou et al and McCarty et al does not explicitly teach overwriting the encrypted portion of the software stored on the writeable storage device by copying the encrypted portion of the software from a read only storage device to a writeable storage device. McCarty discloses a method of overwriting the software by deciphering and re-enciphering with a new key (col 12 ln 22-61). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the combination of Chou et al and McCarty to further overwrite the software stored on the writeable storage device by copying the encrypted portion of the software stored from a read only storage device to a writeable storage device because the applicant has not explicitly stated any particular purpose of such overwriting means other than for providing a software portion encrypted with a second key value and the means of overwriting in the combination of Chou et al and McCarty is just as efficient.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent 6,000,030, to Steinberg et al discloses a method protecting and controlling distribution of software.

US Patent 4,817,140, to Chandra et al discloses a method of software protection.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Allen Wu
Patent Examiner
Art Unit 2135

ASW



Allen S. Wu
Patent Examiner
Art Unit 2135